(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 417 447 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
29.10.1997 Bulletin 1997/44

(51) Int Cl.6: **G06F 1/00**

(21) Application number: **90114545.8**

(22) Date of filing: **28.07.1990**

(54) Data protection by detection of intrusion into electronic assemblies

Datenschutz durch Feststellen von Einbruch in elektronischen Anlagen

Protection de données par détection d'intrusions dans des ensembles électroniques

(84) Designated Contracting States:
DE FR GB IT

(30) Priority: **12.09.1989 US 405910**

(43) Date of publication of application:
20.03.1991 Bulletin 1991/12

(73) Proprietor: **International Business Machines Corporation**
Armonk, N.Y. 10504 (US)

(72) Inventors:
- **Double, Glen Paul**
  Concord, North Carolina 28025 (US)
- **Weingart, Steve Harris**
  Peekskill, New York 10566 (US)

(74) Representative: **Rach, Werner, Dr.**
IBM Deutschland
Informationssysteme GmbH,
Patentwesen und Urheberrecht
70548 Stuttgart (DE)

(56) References cited:
EP-A- 0 142 013
EP-A- 0 268 882
GB-A- 1 201 025
US-A- 4 398 089
US-A- 4 593 384

- **IEEE SYMPOSIUM ON SECURITY AND PRIVACY 27 April 1987, OAKLAND US pages 52 - 58; WEINGART: 'Physical Security for the uABYSS System'**

EP 0 417 447 B1

Printed by Jouve. 75001 PARIS (FR)

adequate over a reasonable period of time to prevent erasure. In still further aspects. the invention includes temp rature sensing means which generates an electrical signal responsive to a temperature which is lower than a predetermined value and which signal is used to cause the erasure of information contained in the memory component, before the temperature of the memory component has reached a temperature low enough to cause a significant number of its storage locations to retain their information even after erasure is attempted.

These aspects of the invention are achieved by the barrier of claim 1.

Description of the Drawings

Fig. 1 is a schematic view of a message encryption/decryption system;

Fig. 2 is a schematic view of the operation of the encryption/decryption system and means to detect and prevent unauthorized interrogation of the system;

Fig. 3 is an exploded perspective view of a circuit card with various devices and components mounted thereon which constitute the system to be protected, and, showing plastic preforms which mate with the card to provide the form-factor for wrapping the flexible screen membrane;

Fig. 4 is a perspective view, somewhat diagrammatic showing a flexible screen member used in this invention;

Fig. 5 is the system of Fig. 3 showing the flexible screen member partially wrapped thereon with screen leads attached to the circuit card;

Fig. 6 is a sectional view taken substantially along the plane of line 6-6 of Fig. 5:

Fig. 7 is a view similar to Fig. 5 in which the screen is wrapped onto the circuit card with parts broken away for clarity;

Fig. 8 is a view similar to Fig. 6 showing the assembly encapsulated in epoxy and contained in a steel container;

Fig. 9 is a sectional view taken substantially along the plane of line 9-9 of Fig. 8:

Fig. 10 is a circuit diagram of a circuit used for detecting mechanical or chemical intrusion through the screen member:

Fig. 11 is a circuit diagram of the circuit used for detecting and obtaining of data by use of high intensity radiation: and

Fig. 12 is a circuit diagram of the circuit used for detecting and preventing obtaining of information by low temperature excursions.

Description of an Embodiment

Referring now to the drawings and for the present to Fig. 1, a conceptual schematic drawing of a message encryption\decryption facility is shown in broken outline 10. The clear message which is to be encrypted is delivered to encryption means 12 which in turn encrypts the clear message via key store 14 to provide an encrypted message. The encryption keys in key store 14 as well as the encryption 12 must be protected from interrogation because if an unauthorized person were to have access to these keys and the encryption process, the clear messages could be derived from encrypted data and misused indiscriminately.

The conceptual block diagram in Fig. 2 shows the scheme of the present invention for detecting and preventing unauthorized interrogation of the stored encryption keys in key store 14. For the purpose of this invention, the encryption keys are retained in a volatile memory 16. The volatile memory 16 is powered by either a battery or system power determined by power switch 18. Power to the memory is controlled by power gate 20 and shorting transistor 21 via detection logic NAND gate 22 which in turn is actuated by sensor circuits designated S, T and X. (Of course, more sensor inputs could be used if desired.) Sensor circuit S, which will be described presently in detail, detects mechanical or chemical intrusion; sensor circuit T, which will be described presently in detail, detects temperature excursions; and sensor circuit X, which will be described presently in detail, detects exposure to radiation. As is well known in the art, the logic NAND gate 22 will normally be in the "low" or "off" condition if all inputs are "on" or "high"; however, if any input goes "low", then the NAND gate output 22 goes "high" providing a signal to other components attached to it. Such a signal from the NAND gate output will cause the power gate 20 to disconnect the memory 16 from power and cause shorting transistor 21 to short the power pin of the memory to ground thus erasing the memory quickly. Thus, if any one of the sensor inputs changes from "high" to "low", as a result of certain predetermined conditions indicating an attack the NAND gate 22 will turn "on" and the data from memory 16 will be quickly erased. Each of these particular detecting circuits will be described presently.

As shown in Fig. 3, a circuit card 24 is provided which contains thereon the various components for encryption, key storage in volatile memory 16. the battery and the protection circuitry for the volatile memory for the encryption/decryption facility 10. The components

36 or 37 is substantially increased or decreased beyond the bounds set by resistor 55. the bias of the operation amplifiers 57 and 58 will change such that one or the other will turn "off" thus changing the input to NAND gate 22 from "high" to "low". As explained previously, this will cause the output of NAND gate 22 to go from "low" to "high", supplying the necessary signal to turn "off" power gate 20 and turn "on" shorting transistor 21 which will quickly erase the information stored in volatile memory 16. The change in resistance of legs 36 or 37 can be due either to breaks or shorts in either of the legs caused by an attempted intrusion, or by a slow change in resistance of the legs 36 or 37 caused by a chemical attack or by other means. Thus, the circuit shown in Fig. 10 will respond to attempted mechanical or chemical intrusions by sending a signal to the NAND gate 22 which in turn will send a signal to cause the erasure of information before the intrusion is complete and the volatile memory can be read.

As indicated previously, there are various special attacks whereby screen barriers can be thwarted, compromised, or by-passed without losing data or memory, if extra precautions are not taken. Two such attacks involve controlled exposure to ionizing radiation and, exposure to low temperatures. The circuitry shown in Fig. 11, detects both visible and ionizing radiation and causes the memory 16 to be erased before ionizing radiation is able to permanently affect the volatile memory. The circuit in Fig. 12 detects temperature excursions below a predetermined value and causes the memory to be erased before a critical low temperature affects the volatile memory.

The circuit for Sensor X, which is responsive to both visible and ionizing radiation is shown in Fig. 11. This circuit includes an operational amplifier 62 having one side connected to diode 63 in series with a resistor 64, the combination of which provides a reference voltage to the positive input of the operational amplifier 62. The negative input of the operational amplifier 62 is connected between a photo sensitive device 65, such as a Photo-Darlington pair or a phototransistor, and resistor 66 to system power or battery via power switch 18 and through resistors 67 to ground. Capacitors 68 and 69 and resistors 66 and 70 have been provided for noise filtering. The photosensitive device is located on the card 24 so that it is not blocked by the lead foil sheets 29, preferably adjacent to the volatile memory chip 16 under the notch 30 of the lead foil sheet such that attempted radiation of this component 16 will also expose the photosensitive device 65 to radiation. In normal operation, the photosensitive device 65 is nonconducting in the absence of radiation and the operational amplifier 62 is biased "on". However, when the photosensitive device senses radiation (either ionizing or in the visible spectrum) of sufficient intensity, it will conduct current which will change the bias on the operational amplifier 62 turning it "off". This will cause the NAND gate 22 to turn "on" and provide a signal to power gate 20 and shorting transistor 21 to cause information stored in volatile memory 16 to be erased as previously described.

The circuitry of Sensor T is shown in Fig. 12. In this circuit three resistors 72, 74 and 76, together with resistor 70, provide the four legs of a bridge circuit, which circuit is connected to operational amplifier 78. Resistor 70 is a thermistor having a negative temperature coefficient of resistance, i.e. its resistance increases with decreasing temperature. The value of the three resistors 72, 74 and 76 are chosen to bias operational amplifier 78 normally "on" within the operating temperature range, and to bias the amplifier "off" at a chosen temperature. The value of resistor 76 is chosen based on the temperature characteristics of thermistor 70. Thus in normal operation the operational amplifier 78 is normally biased "on", but when the temperature falls below a selected low value, e.g. 0°C or -20°C or some other value related to the temperature dependent retention characteristics of volatile memory 16, the operational amplifier 78 will turn "off" which as described above, will cause the NAND gate to give a signal which will cause erasure quickly of the information stored in volatile memory 18.

While one embodiment of this invention has been shown and described various adaptations and modifications may be made without departing from the scope of the invention as defined in the appended claims. For example, the NAND gate can be replaced with other logic circuits performing a logical "or" function to cause erasure of the memory if any one of a number of events are sensed indicating that an intrusion is being attempted. Additional sensors could be used to detect other evidence of intrusion.

Claims

1. A barrier for protecting against intrusions into an electronic assembly comprising:

screen means surrounding said electronic assembly, said screen means including line means (33) formed on a substrate (31) in a pattern, said screen means resisting access without disturbing said line means, said line means being formed of conductive particles (34) of material disposed in a solidified matrix of material, the resistance of said line means changing when said line means are disturbed,

encapsulating material (46) encapsulating said line means and bonded to said line means which bond is stronger than the bond of said line means to said substrate (31) and which encapsulating material is harder and more brittle than said line means, and which ncapsulating material is subject to attack by the same reagents with respect to their chemical properties

wordenen Materialmatrix bestehen, und der Widerstand der Leitungsmittel sich ändert, wenn die Leitungsmittel gestört werden,

ein Einkapselungsmaterial (46), das die Leitungsmittel inkapselt und mit den Leitungsmitteln verbunden (Bondverfahren) ist, wobei diese Verbindung stärker als die Verbindung der Leitungsmittel mit dem Substrat (31) ist, und wobei das Einkapselungsmaterial härter und brüchiger als die Leitungsmittel ist und Angriffen von denselben Reagenzien und ihren chemischen Eigenschaften ausgesetzt ist, die auch das Material der Matrix der Leitungsmittel angreifen;

und ein Stromversorgungs- und Signalerfassungsmittel, das den Leitungsmitteln ein Eingangssignal bereitstellt und ein Ausgangssignal erzeugt, wenn der Widerstand der Leitungsmittel sich ändert.

2. Eine Schutzsperre nach Anspruch 1, bei der die elektronische Anlage ein flüchtiges Speichermittel umfaßt, und bei der auf das Ausgangssignal reagierende Mittel bereitgestellt werden, um die im flüchtigen Speichermittel gespeicherten Daten zu löschen.

3. Eine Schutzsperre nach Anspruch 1 oder 2, bei der die Leitungsmittel weiterhin zahlreiche Leitungssegmente umfassen, und bei der das Stromversorgungs- und Erfassungsmittel Widerstandsänderungen zwischen zwei Leitungssegmenten erfaßt.

4. Eine Schutzsperre nach Anspruch 3, bei der die Leitungsmittel einen Teil einer Spannungsteilerschaltung bilden.

5. Eine Schutzsperre nach Anspruch 4, bei der Mittel bereitgestellt werden, um das Ausgangssignal zu erzeugen, das auf die Widerstandsänderung der Leitungssegmente in der Spannungsteilerschaltung reagiert.

6. Eine Schutzsperre nach Anspruch 5, bei der das Ausgangssignal durch ein Verstärkermittel erzeugt wird, das an die Spannungsteilerschaltung angeschlossen ist.

7. Eine Schutzsperre nach einem der Ansprüche 1 bis 6, die weiterhin ein Mittel zum Erfassen einer unter einem gegebenen Temperaturwert liegenden Temperatur und zum Erzeugen eines Ausgangssignals umfaßt, das auf die Erfassung der Temperaturabweichung reagiert.

8. Eine Schutzsperre nach einem der Ansprüche 1 bis 6, die weiterhin ein Mittel zum Erfassen von Strahlung über einem gegebenen Wert und zum Erzeugen eines Ausgangssignals umfaßt, das auf die erfaßte Strahlung reagiert.

9. Eine Schutzsperre nach einem der Ansprüche 1 bis 6, die weiterhin ein Mittel zum Erfassen einer unter einem gegebenen Temperaturwert liegenden Temperatur und zum Erzeugen eines Ausgangssignals umfaßt, das auf die Erfassung der Temperaturabweichung reagiert, sowie ein Mittel zum Erfassen von Strahlung über einem gegebenen Wert und zum Erzeugen eines Ausgangssignals, das auf die erfaßte Strahlung reagiert.

10. Eine Schutzsperre nach Anspruch 7 oder 9, bei der das Mittel zum Erfassen der Temperaturabweichung ein Schaltungsmittel mit einem Mittel zum Bereitstellen eines Bezugssignals umfaßt, um die Reaktion auf die Temperaturabweichung zu steuern.

11. Eine Schutzsperre nach Anspruch 10, bei der das Schaltungsmittel ein temperaturempfindliches Widerstandsmittel umfaßt, das seine Ausgaben in Abhängigkeit von der Temperatur verändert.

12. Eine Schutzsperre nach Anspruch 11, bei der das Schaltungsmittel eine Bezugsbrückenschaltung ist.

13. Eine Schutzsperre nach Anspruch 11 oder 12, bei der das Ausgangssignal von einem Verstärker erzeugt wird, der mit dem Schaltungsmittel verbunden ist.

14. Eine Schutzsperre nach Anspruch 8 oder 9, bei der das Mittel zum Erfassen der Strahlung ein Schaltungsmittel mit einem Mittel, insbesondere einer strahlungsempfindlichen Vorrichtung, umfaßt, um ein Merkmal zu ändern, das auf die erfaßte Strahlung reagiert.

15. Eine Schutzsperre nach Anspruch 14, bei der das Schaltungsmittel einen operationsverstärker umfaßt, der das Ausgangssignal erzeugt.

16. Eine Schutzsperre nach einem der oben genannten Ansprüche 8, 9, 14 oder 15, die weiterhin ein Strahlungsabschirmmittel umfaßt, um die vom flüchtigen Speicher empfangene Strahlung verglichen mit der vom Strahlungserfassungsmittel empfangenen Strahlung zu verringern.

17. Eine Schutzsperre nach einem der Ansprüche 2-16, bei der Gattermittel bereitgestellt werden, um das Ausgangssignal zu erzeugen, und/oder Schaltmittel, um den Strom für den flüchtigen Speicher, der auf das Ausgangssignal reagiert, abzuschalten.

par un amplificateur relié audit moyen de circuit.

14. Barrière de protection selon la revendication 8 ou 9, dans laquelle ledit moyen destiné à détecter un rayonnement comprend un moyen de circuit comportant un moyen, en particulier un dispositif photosensible, afin de faire varier une caractéristique de celui-ci en réponse audit rayonnement détecté.

15. Barrière de protection selon la revendication 14, dans laquelle ledit moyen de circuit comprend un amplificateur opérationnel qui produit ledit signal de sortie.

16. Barrière de protection selon l'une quelconque des revendications précédentes 8, 9, 14 ou 15, comprenant en outre un moyen de blindage contre les rayonnements disposé pour réduire le rayonnement reçu par ladite mémoire volatile par rapport aux rayonnements reçus par ledit moyen destiné à détecter un rayonnement.

17. Barrière de protection selon l'une quelconque des revendications 2 à 16, dans laquelle un moyen de porte est prévu pour générer ledit signal de sortie, et/ou un moyen d'interrupteur destiné à couper l'alimentation vers ladite mémoire volatile en réponse au signal de sortie.

18. Barrière de protection selon la revendication 17, comprenant en outre un moyen de transistor destiné à court-circuiter ladite mémoire volatile en réponse audit signal de sortie.

19. Barrière de protection selon l'une quelconque des revendications 2 à 18, comprenant en outre un moyen destiné à procurer un blindage contre les interférences électromagnétiques.

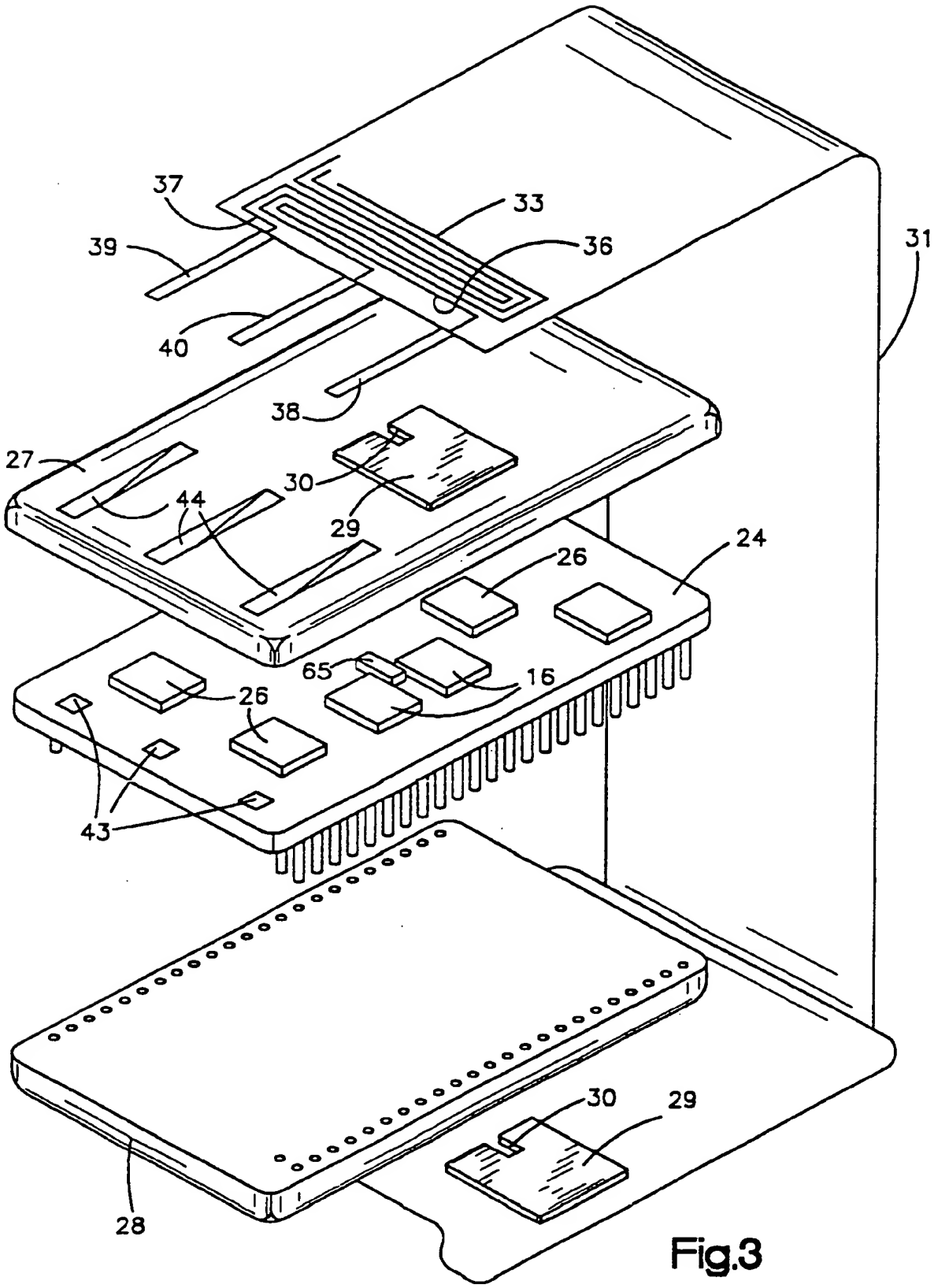

Fig.3

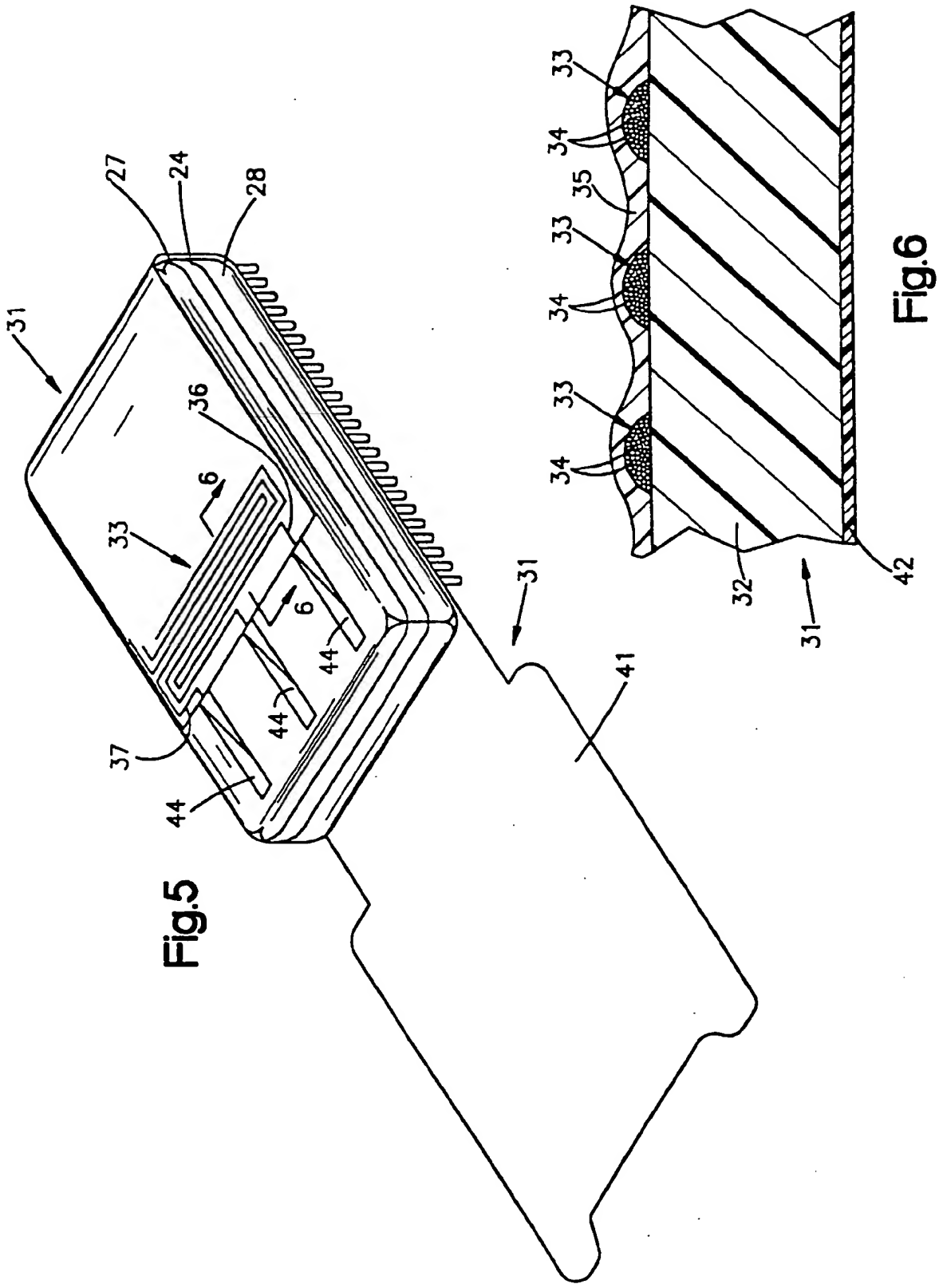

Fig.5

Fig.6

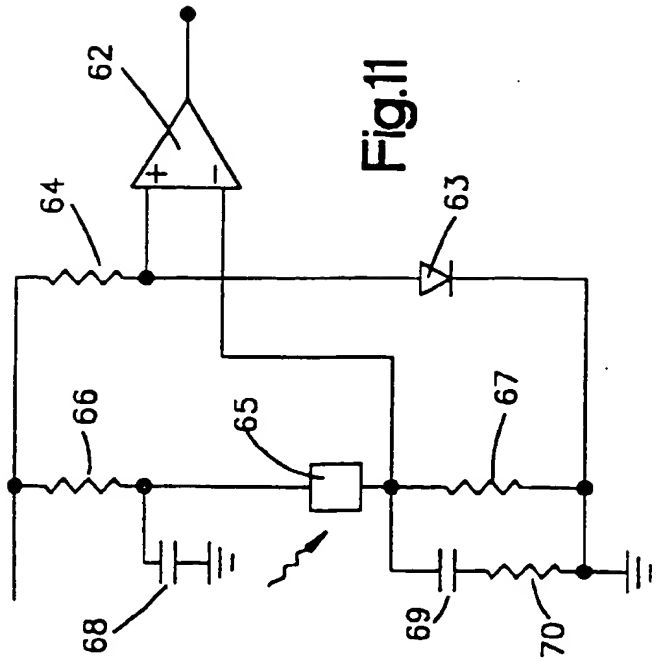

Fig.11

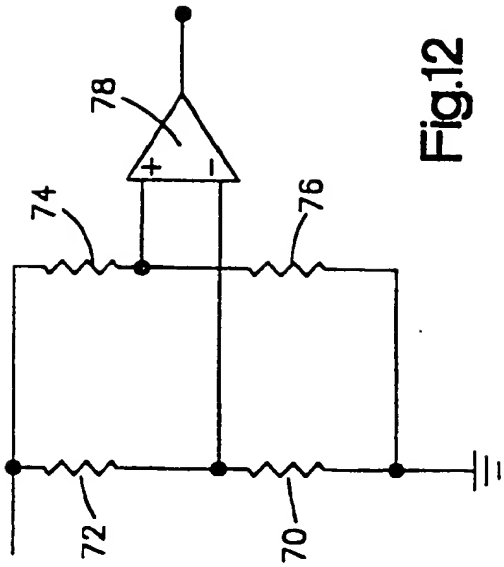

Fig.12

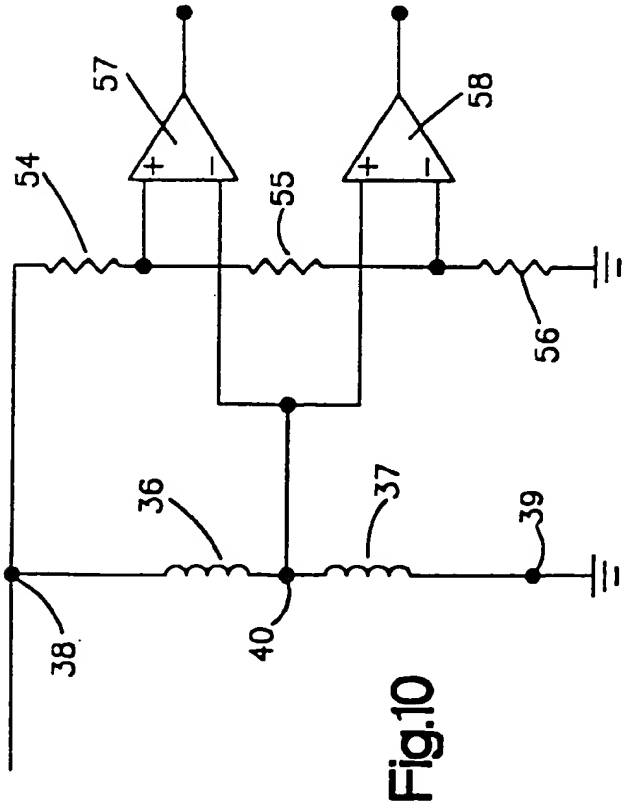

Fig.10